UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/022,578	12/17/2001	Bhaskar Sinha	ONET-0101 PUS	6146

27256 7590 04/07/2006

ARTZ & ARTZ, P.C.
28333 TELEGRAPH RD.
SUITE 250
SOUTHFIELD, MI 48034

EXAMINER	
POPHAM, JEFFREY D	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 04/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/022,578	SINHA ET AL.	
	Examiner	Art Unit	
	Jeffrey D. Popham	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 March 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 December 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Remarks

Claims 1-23 are pending.

Response to Arguments

1. Applicant's request for reconsideration of the finality of the rejection of the last Office action is persuasive and, therefore, the finality of that action is withdrawn. As discussed in the previous office action, the specification discloses that encrypting and decrypting a piece of data "with a ticket" comprises using a password (or symmetric key, as is also disclosed in the specification). Applicant's arguments with respect to claims 1-23 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. The claims are still rejected under 35 U.S.C. 112, second paragraph.

The issues in claim 12 were not fixed, even though they were given as examples in the previous office action. Claims 10 and 11 have problems, such as the only authentication within claim 8 being at the head end server, but claim 10 now claims that the (only) step of authentication is performed within a policy engine, that is within the privilege server. Claim 11 generates a ticket by encrypting the non-generated ticket. This is rather impossible. Those are the major issues, but there are, of course, others, such as not using consistent language (i.e. user

privilege server proxy being called different things throughout), changing something in one claim but not another which had the same exact limitation (claim 1 was amended to change "user identification" to "user information", claim 8 was not, even though it is the same exact problem).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-4 and 13-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jerdonek (U.S. Patent Application Publication 2002/0095507) in view of Sampson (U.S. Patent 6,490,624) and Lim (U.S. Patent 6,728,884).

Regarding Claim 1,

Jerdonek discloses a method of authenticating a user having a user privilege server proxy for a network system having a privilege server, a head end server and a web adapter comprising:

Presenting user information to the web adapter from the user privilege sever proxy (Paragraphs 45, 46, and 63);

Presenting the user information to the head end server (Paragraphs 45, 46, and 63);

Presenting the user information to the privilege server from the head end server (Paragraphs 45, 46, and 63);

Validating the user in response to the user information (Paragraph 47; there is some validation due to the password being pre-authorized, in this context);

When a user is validated, generating a ticket for the user at the privilege server (Paragraph 47);

Providing the ticket to the user privilege server proxy through the head end server (Paragraphs 48, 49, and 63);

Forming a service access request token from the ticket and the user information (Paragraph 49);

Sending the token from the user to the privilege server (Paragraph 50);

Validating the user in response to the token (Paragraphs 51-53);

Forming a packet having a sequence number, session key and the ticket (Paragraphs 45, 46, and 56);

Providing the packet to the head end server (Paragraphs 56 and 63);

In response to receiving the packet, authenticating the user at the head end server (Paragraphs 45, 46, 56, and 63);

Providing the packet to the user privilege server proxy (Paragraph 56);

Sending the ticket and sequence number encrypted with the session key to a service server through the web adapter (Paragraph 58);

Validating the user for the service server (Paragraph 59); and

Granting the user privileges at the service server (Paragraph 60);

But does not explicitly disclose that forming the packet is done at the privilege server, validating the user at the service server, or that the privileges are role based.

Sampson, however, discloses that forming the packet is done at the privilege server (Abstract). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the session management system of Sampson into the authentication system of Jerdonek in order to provide an improved way to manage sessions in networks that use stateless protocols.

Lim, however, discloses validating the user at the service server (Column 8, lines 16-33); and that the privileges are role based (Column 3, lines 41-57; and Column 4, lines 49-60). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the access control system of Lim into the authentication system of Jerdonek as modified by Sampson in order to provide a mechanism by which to govern access to particular users that is easy to reconfigure as new user applications and authentication techniques become available.

Regarding Claim 13,

Claim 13 is a system claim that is broader than method claim 8 and is rejected for the same reasons.

Regarding Claim 14,

Claim 14 is a system claim that is broader than method claim 8 and is rejected for the same reasons.

Regarding Claim 22,

Claim 22 is a system claim that is broader than method claim 8 and is rejected for the same reasons.

Regarding Claim 2,

Jerdonek as modified by Sampson and Lim discloses the method of claim 1, in addition, Lim discloses negotiating an authentication scheme between the server proxy and privilege server (Column 5, lines 18-44).

Regarding Claim 3,

Jerdonek as modified by Sampson and Lim discloses the method of claim 2, in addition, Lim discloses that negotiating the authentication scheme between the user privilege server proxy and privilege server comprises presenting at least one security mechanism from the user privilege server proxy to the privilege server; accepting or rejecting the at least one security mechanism at the privilege server (Column 5, lines 18-44).

Regarding Claim 4,

Jerdonek as modified by Sampson and Lim discloses the method of claim 2, in addition, Lim discloses that the step of validating the user in response to the user information comprises validating the user in response to the user information in accordance with the authentication scheme (Column 5, lines 18-44).

Regarding Claim 15,

Jerdonek as modified by Sampson and Lim discloses the system of claim 13, in addition, Jerdonek discloses that the user information comprises a user identification number (Paragraph 45).

Regarding Claim 16,

Jerdonek as modified by Sampson and Lim discloses the system of claim 13, in addition, Jerdonek discloses that the privilege server has a policy engine therein (Paragraphs 45-49).

Regarding Claim 17,

Jerdonek as modified by Sampson and Lim discloses the system of claim 16, in addition, Jerdonek discloses that the privilege server comprises a key generator coupled to the policy engine (Paragraphs 45-49).

Regarding Claim 18,

Jerdonek as modified by Sampson and Lim discloses the system of claim 16, in addition, Lim discloses that the privilege server comprises a proxy coordinator coupled to the policy engine (Column 6, lines 11-22).

Regarding Claim 19,

Jerdonek as modified by Sampson and Lim discloses the system of claim 16, in addition, Jerdonek discloses that the privilege server comprises an obfuscator/deobfuscator coupled to the policy engine (Paragraphs 45 and 46).

Regarding Claim 20,

Jerdonek as modified by Sampson and Lim discloses the system of claim 16, in addition, Jerdonek discloses that the privilege server comprises a store keeper coupled to the policy engine (Paragraphs 52-59).

Regarding Claim 21,

Jerdonek as modified by Sampson and Lim discloses the system of claim 20, in addition, Jerdonek discloses that the store keeper comprises a user information list and a session information list (Paragraphs 52-59).

4. Claims 5-12 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jerdonek in view of Sampson and Lim, further in view of Menezes (Menezes et al., "Handbook of Applied Cryptography", 1997, pp. 15-21 and 31).

Regarding Claim 5,

Jerdonek as modified by Sampson and Lim discloses the method of claim 1, in addition, Jerdonek discloses that the data is a ticket (Paragraph

47); but does not disclose the step of encrypting the data with a user password to form an encrypted data.

Menezes, however, discloses the step of encrypting the data with a user password to form an encrypted data (Pages 15-21). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the symmetric encryption technique of Menezes into the authentication system of Jerdonek as modified by Sampson and Lim in order to provide a way to secure data that is fast, has short keys, and cannot be decrypted without the password.

Regarding Claim 6,

Jerdonek as modified by Sampson, Lim, and Menezes discloses the method of claim 5, in addition, Menezes discloses the step of decrypting the encrypted data (Pages 15-21); and Jerdonek discloses that this is done at the user privilege server proxy (Paragraphs 47-49).

Regarding Claim 7,

Jerdonek as modified by Sampson and Lim discloses the method of claim 1, in addition, Jerdonek discloses that a packet has a sequence number, session key, and ticket (Paragraphs 45 and 46) and that the packet is received by the user privilege server proxy (Paragraph 56), and Sampson discloses that a packet is formed at the privilege server (Abstract); but does not disclose that data is encrypted with the ticket

(which, as discussed in the previous office action, is encrypted with the user's password) and decrypted with the same.

Menezes, however, discloses that data is encrypted with the ticket (with a password) and decrypted with the ticket (the same password) (Pages 15-21). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the symmetric encryption technique of Menezes into the authentication system of Jerdonek as modified by Sampson and Lim in order to provide a way to secure data that is fast, has short keys, and cannot be decrypted without the password.

Regarding Claim 8,

Jerdonek discloses a method of authenticating a user having a user privilege server proxy for a network system having a privilege server, a head end server and a web adapter comprising:

Presenting user information to the web adapter (Paragraphs 45, 46, and 63);

Presenting the user information to the head end server (Paragraphs 45, 46, and 63);

Presenting the user information to the privilege server from the head end server (Paragraphs 45, 46, and 63);

Validating the user in response to the user information (Paragraph 47);

When a user is validated, generating a ticket for the user at the privilege server (Paragraph 47);

Providing the ticket to the user privilege server proxy through the head end server (Paragraphs 48, 49, and 63);

Forming a service access request token from the ticket and the user information at the user privilege server proxy (Paragraph 49);

Sending the token from the user privilege server proxy to the privilege server (Paragraph 50);

Validating the user in response to the token (Paragraphs 51-53);

Forming a packet having a sequence number, session key and the ticket (Paragraphs 45, 46, and 56);

Providing the packet to the head end server (Paragraphs 56 and 63);

In response to receiving the packet, authenticating the user at the head end server (Paragraphs 45, 46, 56, and 63);

Providing the packet to the user privilege proxy (Paragraph 56);

Sending the ticket and sequence number encrypted with the session key to a service server through the web adapter (Paragraph 58);

Validating the user for the service server (Paragraph 59); and

Granting the user privileges at the service server (Paragraph 60).

Sampson, however, discloses that forming the packet is done at the privilege server (Abstract). It would have been obvious to one of ordinary

skill in the art at the time of applicant's invention to incorporate the session management system of Sampson into the authentication system of Jerdonek in order to provide an improved way to manage sessions in networks that use stateless protocols.

Lim, however, discloses negotiating an authentication scheme between the server proxy and privilege server (Column 5, lines 18-44); the step of validating the user in response to the user information comprises validating the user in response to the user information in accordance with the authentication scheme (Column 5, lines 18-44); validating the user at the service server (Column 8, lines 16-33); and that the privileges are role based (Column 3, lines 41-57; and Column 4, lines 49-60). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the access control system of Lim into the authentication system of Jerdonek as modified by Sampson in order to provide a mechanism by which to govern access to particular users that is easy to reconfigure as new user applications and authentication techniques become available.

Menezes, however, discloses the step of encrypting the data with a user password to form an encrypted data (Pages 15-21); the step of decrypting the encrypted data (Pages 15-21); and that data is encrypted with the ticket (with a password) and decrypted with the ticket (the same password) (Pages 15-21). It would have been obvious to one of ordinary

skill in the art at the time of applicant's invention to incorporate the symmetric encryption technique of Menezes into the authentication system of Jerdonek as modified by Sampson and Lim in order to provide a way to secure data that is fast, has short keys, and cannot be decrypted without the password.

Regarding Claim 23,

Claim 23 is a method claim that is broader than method claim 8 and is rejected for the same reasons.

Regarding Claim 9,

Jerdonek as modified by Sampson, Lim, and Menezes discloses the method of claim 8, in addition, Lim discloses that negotiating the authentication scheme between the server proxy and privilege server comprises presenting at least one security mechanism from the user privilege server proxy to the privilege server and accepting or rejecting the at least one security mechanism at the privilege server (Column 5, lines 18-44).

Regarding Claim 10,

Jerdonek as modified by Sampson, Lim, and Menezes discloses the method of claim 8, in addition, Jerdonek discloses that a step of validation is performed by a policy engine within the privilege server (Paragraphs 47, 51-53, and 59).

Regarding Claim 11,

Jerdonek as modified by Sampson, Lim, and Menezes discloses the method of claim 8, in addition, Jerdonek discloses that generating a ticket comprises generating the ticket and, once the ticket is generated, encrypting the ticket with a session key (Paragraphs 45-49).

Regarding Claim 12,

Claim 12 is a method claim that is broader than method claim 8, except for the steps of including a session name and choosing a service in the service server. Lim discloses including a session name (Column 8, lines 16-33) and choosing a service in the service server (Column 3, lines 41-57).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey D. Popham whose telephone number is (571)-272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jeffrey D Popham
Examiner
Art Unit 2137

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER